



*FISMA Fact – “Each federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support operations and assets of the agency, including those provided or managed by another agency, contractor, or other source...”*

– Federal Information Security Management Act of 2002

IT systems; (2) the DON Plan of Action and Milestones (POA&M); and (3) the status of information systems privacy management.

The Secretary of the Navy directed the DON to reach and sustain 90 percent or greater certification and accreditation status for DON systems and networks. This C&A compliance rate is required by the President’s Management Agenda for 2005.

OMB requires federal agency CIOs to monitor the status of information security weaknesses, including the lack of full accreditation in POA&Ms for each system and network. OMB reviews POA&Ms for systems for which a Capital Asset Plan and Justifications (known as OMB Exhibit 300) is submitted. The Department of the Navy Chief Information Officer (DON CIO) retains other system POA&Ms and provides a summary report to OSD quarterly.

The DON CIO is responsible for DON compliance with Section 208, Privacy Provisions of the E-Government Act of 2002. OMB Memorandum 03-22, “Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,” issued Sept. 26, 2003, provides OMB requirements for compliance with the E-Government Act and states the conditions in which a Privacy Impact Assessment is required for an IT system. The DON CIO has developed a Privacy Impact Assessment, which is available on the DON CIO Web site. (*See the Reference Links box for information.*)

In fiscal year 2005, OMB introduced a new privacy management section of FISMA reporting, which removes privacy compliance reporting from the annual E-Government Act report to the annual FISMA report.

### OMB FISMA Guidance for FY 2005

In 2005, OMB issued M-05-15, “FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management” to facilitate FISMA reporting. This memorandum provides reporting instructions and FISMA and Privacy Management reporting templates.

FISMA requires system owners to annually review certification and accreditation status of all systems, including those that are accredited (i.e., granted an approval to operate). This annual review must include all items listed in DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” issued Feb. 6, 2003.

FISMA requires that certification and accreditation statistics for contractor and government systems be reported separately. Contractor systems are information systems used or operated by a contractor of a federal agency or other organization on behalf of the agency. An example of a contractor system is the Navy Marine Corps Intranet.

### FISMA Fundamentals

The Department of the Navy (DON) is required to comply with the Federal Information Security Management Act of 2002 (FISMA) also known as Title III of the E-Government Act of 2002. FISMA requires each federal agency to provide information security for its information technology (IT) assets. The purpose of FISMA is to provide a framework for enhancing the effectiveness of information security in the federal government. FISMA also provides a mechanism for effective oversight of federal agency information security programs.

The director of the Office of Management and Budget (OMB) oversees FISMA compliance. The DON reports FISMA status to the Assistant Secretary of Defense (Networks and Information Integration) (ASD/NII), which consolidates all Department of Defense (DoD) input and reports to OMB. This article explains the importance of accurate and timely reporting of FISMA data.

### FISMA Reporting Using the IT Registry

The DoD Information Technology Registry serves as a technical repository to support chief information officers’ (CIO) assessments and maintains an IT system inventory to comply with Congressional requirements. The Office of the Secretary of Defense (OSD) uses data from the DoD IT Registry to compile reports regarding FISMA status.

The DON uses its own DON IT Registry to record the certification and accreditation (C&A) status of mission critical (MC), mission essential (ME), and mission support (MS) DON systems and networks. The DON uploads this data quarterly (March 1, June 1, Sept. 1 and Dec. 1) into the DoD IT Registry. Data from the DoD IT Registry is used to report FISMA status for the entire DoD to OMB and Congress. The DON must improve the recording and reporting of IT systems data to increase compliance with OSD and OMB FISMA requirements. Punctual and accurate reporting of DON IT systems is key to validating DON compliance with security requirements and justifying funding for IT security tasks.

### Key Issues for FISMA Compliance

Three key areas of FISMA compliance that affect the DON are: (1) reporting the certification and accreditation status of DON

## DoD FISMA Guidance for FY 2005

In addition to the OMB requirements for 2005, the Office of the Secretary of Defense issued FISMA guidance to assist the DoD in complying with the new requirements. There is a new requirement for system owners to report the status of mission support IT systems in the DoD IT Registry, in addition to the current requirement to report mission critical and mission essential systems. With this new requirement OSD seeks to comply with the President's Management Agenda and the E-Government Act, both of which mandate that all systems be registered in the DoD IT Registry.

DoD FISMA Guidance for FY05 requires submission of quarterly Plan of Action and Milestones to OSD for the number and category of information security POA&Ms and for activities leading up to accreditation for:

- ✓ Exhibit 300 systems that are not fully accredited.
- ✓ Exhibit 300 systems that receive a security score of three or lower on a scale of one to five.
- ✓ Systems in the IT Registry that require certification and accreditation, but do not have an approval to operate.
- ✓ Systems with material weaknesses or significant deficiency in the DON's information security posture. These items might be identified in an audit or by internal review.

OSD is updating this guidance and it should be issued in fall 2005. The new guidance will be posted on the DON CIO Web site when it becomes available.

The Office of the Secretary of Defense develops and reports summary data from all POA&Ms reported to the DoD, to OMB and Congress in the annual DoD FISMA Enterprise Plan of Action & Milestones. DoD and DON POA&M guidance is based on OMB Memorandum M-04-25, "FY 2004 Reporting Instructions for FISMA." OSD mandated that all defense agencies and military departments must register all mission critical, mission essential and mission support systems in their respective IT registries and report the status of these systems to OSD by Sept. 1, 2006.

The "DON FY 2005 Information Technology (IT) Registration Database Guidance" provides details on what must be entered in the database and who is responsible for entering it.

## DON FISMA Reporting Responsibilities

FISMA reporting is required at all levels of the DON.

- The DON CIO, Mr. David Wennergren, reports DON FISMA status to OSD, and provides supplemental reporting information to the DON Privacy Act Official in support of the DON privacy management reporting section of FISMA.
- The DON Deputy CIO for Policy and Integration, Mr. Robert Carey, is the DON Senior Information Assurance Official. He is responsible for the DON information security program.
- Program Managers, System Managers, Command Information Officers, and Functional Area Managers are responsible for updating the FISMA data in the DON IT Registry.

## Dates to Remember

Oct. 7, 2005 – FY 2005 Annual FISMA Report due to OMB.

March 1, June 1, Sept. 1 and Dec. 1 – Agency CIOs are required by law to report quarterly to OMB with POA&M status. OSD forwards the data to OMB on the 15th of these months.

Sept 1, 2006 – The OSD requires the DON to upload all of its certification and accreditation data on mission support systems into the DoD IT Registry by this date.

Oct. 15 – DON CIO certifies with DoD CIO that the DON IT Registry data are accurate and complete.

## Reference Links

Subchapter III of Chapter 35 of Title 44, U. S. Code, "Federal Information Security Management Act (FISMA) of 2002" (PL 107-347). Web link: <http://csrc.nist.gov/policies/FISMA-final.pdf>.

Section 208, Privacy Provisions, of the E-Government Act of 2002. Web link: <http://www.whitehouse.gov/omb/memoranda/m03-22.html/> and scroll to Attachment B.

OMB Memorandum M-03-22, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," of Sept. 26, 2003. Web link: <http://www.whitehouse.gov/omb/memoranda/m03-22.html/>.

OMB Memorandum M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," of Aug. 23, 2004. Web link: <http://www.whitehouse.gov/omb/memoranda/fy04/m04-25.pdf>.

OMB Memorandum M-05-15, "FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," of June 13, 2005. Web link: <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-15.html/>.

DON FY2005 IT Registration Database Guidance, March 2005. Web link: <http://www.doncio.navy.mil> and search for "IT Registration."

DON Privacy Impact Assessment Summary Version 1.1. Web link: <http://www.doncio.navy.mil> and search for "Privacy Impact Assessment."

## Compliance is Mandatory

DON compliance with FISMA requirements is mandatory and ensures that the Department performs due diligence in gathering and reporting data on the security of its IT systems. The timely and accurate reporting of DON FISMA data to DoD and OMB is essential to demonstrating the DON IA posture. FISMA requirements change, and the DON must remain vigilant of the new requirements each year to ensure compliance.

*Jennifer Korenblatt is a contractor supporting the DON CIO Information Assurance Team.*

CHIPS